IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Messaoud Benantar		
Assignee:	International Business Machines Corporation		
Title:	Method and System for Public-Key-Based Secure Authentication to Distributed Legacy Applications		
Serial No.:	09/821,079	Filing Date:	March 29, 2001
Examiner:	Christopher J. Brown	Group Art Unit:	2134
Docket No.:	AUS920010064US1	Customer No.	65362

Austin, Texas
May 16, 2008

FILED ELECTRONICALLY

APPEAL BRIEF UNDER 37 CFR § 41.37

Dear Sir:

Applicant submits this Appeal Brief pursuant to the Notice of Appeal filed in this case on March 3, 2008. The fee for this Appeal Brief is being paid electronically via the USPTO EFS. The Board is authorized to deduct any other amounts required for this appeal brief and to credit any amounts overpaid to Deposit Account No. 09-0447.

I. REAL PARTY IN INTEREST - 37 CFR § 41.37(c)(1)(i)

The real party in interest is the assignee, International Business Machines Corporation, as named in the caption above and as evidenced by the assignment set forth at Reel 011685, Frame 0469.

II. RELATED APPEALS AND INTERFERENCES - 37 CFR § 41.37(c)(1)(ii)

Based on information and belief, there are no appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the Board of Patent Appeals and Interferences in the pending appeal. Pursuant to current Patent Office practice, Appendix "A" contains copies of all decisions rendered by a court or the Board in this "Related Appeals and Interferences" section, and is intentionally provided as an empty appendix.

III. STATUS OF CLAIMS - 37 CFR § 41.37(c)(1)(iii)

Claims 1-7, 14-20, and 25-31 are pending in the application. Claims 1-7, 14-20, and 25-31 stand rejected. Claims 8-13, 21-24, and 32-35 have been canceled without prejudice. The rejection of claims 1-7, 14-20, and 25-31 is appealed. Appendix "B" contains the full set of pending claims.

IV. STATUS OF AMENDMENTS - 37 CFR § 41.37(c)(1)(iv)

Claims 8-13, 21-24, and 32-35 were canceled in a Response to Restriction Requirement filed February 28, 2007. In response to the Office Action dated May 15, 2007, Applicant amended claims 1, 14, and 25. In the Final Office Action dated November 1, 2007, the Examiner entered a new ground of rejection.

V. SUMMARY OF CLAIMED SUBJECT MATTER - 37 CFR § 41.37(c)(1)(v)

The subject matter defined in the claims may be understood with reference to the example embodiments depicted in Figures 1 and 5-7 which depict a method, apparatus, and a computer program product for authenticating a client seeking to access a controlled resource. A host application or system (e.g., application server 500) within a distributed data processing system supports one or more controlled resources 526, such as a legacy application, that requires the receipt of authentication data prior to allowing a user to have access to the controlled resource. The required authentication data is encrypted using the public key of the host system, and an attribute certificate containing the encrypted authentication data is generated by an attribute-certificate-issuing authority. *See*, *e.g.*, Application, ¶¶ 75-77. When a user of a client application or system requires access to the controlled resource, the attribute certificate is sent to the host, which decrypts the authentication data with its private key prior to forwarding the authentication data to the controlled resource. *See*, *e.g.*, Application, ¶¶ 79-80, 86-89. The controlled resource then authenticates a user based on the provided authentication data. *See*, *e.g.*, Application, ¶ 89.

To comply with 37 CFR § 41.37(c)(1)(v), a color-coded comparison of independent claim 1 and Figure 7 is now provided to explain how the subject matter defined in the claims may be understood with reference to the example embodiment depicted in Figure 7 which depicts an authentication process methodology within a distributed data processing system (e.g. distributed data processing system 100 depicted in Figure 1). In the disclosed methodology, **an attribute certificate from a client is received at a host within the distributed data processing system (step 702)**. In response, the host extracts encrypted authentication data from the

attribute certificate, where the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host (step 704). Upon extracting the encrypted authentication data, the host then decrypts the encrypted authentication data to regenerate the authentication data using a private key associated with the host (steps 706, 708). **The host then forwards the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource (step 710).**

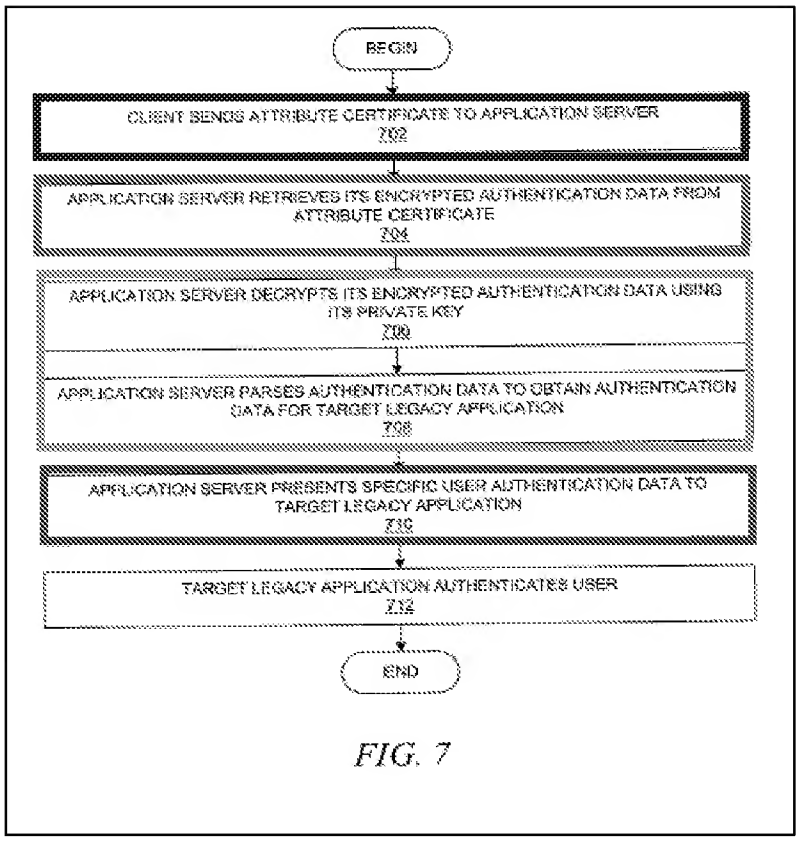


FIG. 7

In further compliance with 37 CFR § 41.37(c)(1)(v), a color-coded comparison of selected Figures from the application and each of the pending independent claims is attached at Appendix "C" to provide a concise explanation of the subject matter defined in each independent claim. The subject matter of the independent claims is set forth in the specification at U.S. Patent Pub. No. 20020144108, ¶ 12 (page 5, lines 1-20), ¶¶ 71-95 (page 26, line 7 to page 35, line 16), and the Abstract (page 49, lines 1-24), though additional contextual description is provided in the application along with the originally-filed claims. For example, the subject matter of claim 1 maps to Figure 7 (see above) and to the specification at paragraph 12 (page 5, lines 1-20), paragraphs 79-80 (page 29, line 22 to page 30, line 9), and paragraphs 86-95 (page 32, line 3 to page 35, line 16); the subject matter of claim 14 maps to Figures 5 and 7 and to the specification at paragraph 12 (page 5, lines 1-20), paragraphs 71-80 (page 26, line 7 to page 30, line 9), and paragraphs 86-95 (page 32, line 3 to page 35, line 16); and the subject matter of claim 25 maps to Figures 5 and 7 and to the specification at paragraph 12 (page 5, lines 1-20), paragraphs 71-80 (page 26, line 7 to page 30, line 9), and paragraphs 86-95 (page 32, line 3 to page 35, line 16). While Applicant has identified passages from the specification to explain the independent claim subject matter, it will be appreciated that the referenced description includes

contextual information to provide an overall context for an example embodiments, and therefore should not be used to improperly read limitations from the specification into the claims.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In the final Office Action dated November 1, 2007, the Examiner withdrew the previous rejection, but a new ground of rejection was asserted for rejecting pending claims 1-7, 14-20 and 25-31. In particular, claims 1, 3-6, 14, 16-19, 25, and 27-30 were rejected as obvious over U.S. Patent No. 6,892,307 to Wood in view of U.S. Patent No. 5,892,828 to Perlman; claims 2, 15 and 26 were rejected as obvious over Wood and Perlman in view of U.S. Patent No. 6,460,141 to Olden; and claims 7, 20 and 31 were rejected as obvious over Wood and Perlman in view of U.S. Patent No. 6,754,829 to Butt. Accordingly, the grounds of rejection that are on appeal are:

(A) the rejection of claims 1, 3-6, 14, 16-19, 25, and 27-30 over Wood in view of Perlman,

(B) the rejection of claims 2, 15, and 26 over Wood in view of Perlman and Olden; and

(C) the rejection of claims 7, 20, and 31 over Wood in view of Perlman and Butt.

VII. ARGUMENTS

A. Claims 1, 3-6, 14, 16-19, 25 and 27-30 Are Not Obvious Over Wood and Perlman

Applicant appeals the Examiner's rejection of claims 1, 3-6, 14, 16-19, 25 and 27-30 as being obvious over Wood in view of Perlman, and respectfully requests reconsideration and withdrawal of the rejection because the Examiner has not established a *prima facie* case of obviousness. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Where a rejection is based on the assertion that all claim limitations are found in a number of prior art references, the fact finder must determine "[w]hat the prior art teaches, whether it teaches away from the claimed invention, and whether it motivates a combination of teachings from different references." In re Fulton, 391 F.3d 1195, 1199-1200 (Fed. Cir. 2004).

As a preliminary matter, a *prima facie* case of obviousness has not been established because, as noted above, none of the references, alone or in combination, discloses or suggests authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract and decrypt

authentication data from the client that is then forwarded to the controlled resource for authenticating the client, as variously recited in claims 1, 14 and 25. *See, e.g.*, claim 1 ("forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.") and Application, Abstract. In particular, the Examiner appears to combine and conflate the host-based claim requirements of "extracting encrypted authentication data from the attribute certificate…" and "decrypting the encrypted authentication data to regenerate the authentication data." According to the Examiner, both of these requirements are met by Wood's description of "decrypting" (Wood, col. 18, lines 54-55). *See*, Final Office Action, pp. 2-3. While Applicant agrees that Wood discloses decrypting the encrypted login credentials, Applicant respectfully submits that the cited "decrypting" disclosure fails to meet the two, distinct claim requirements of "extracting encrypted authentication data from the attribute certificate…" and "decrypting the encrypted authentication data to regenerate the authentication data." At best, Wood discloses decrypting the encrypted login credentials (which, according to the Examiner, corresponds to the claimed "attribute certificate" requirement), but does not separately disclose decrypting encrypted authentication data that has been extracted from the attribute certificate/login credential.

In addition to the foregoing, the Examiner has conceded that "Woods fails to teach forwarding the authentication data to a controlled resource." Final Office Action, p. 3. The disclosure from Perlman cited by the Examiner (Perlman, Application Server 236 at Server Node 202b, col. 6, lines 28-35) to meet the "forwarding" claim requirement is likewise deficient, insofar as the information (e.g., the decrypted "application secret") forwarded to Perlman's "server node 202b" is not provided by an authenticating host that is separate from the client/user, but is actually provided by the user/workstation 210 directly! Rather than routing the authentication operations through a host (as claimed), Perlman discloses the following sequence: (1) the user/workstation 210 attempts to access the application 236; (2) in response, the application 236 issues an authentication inquiry to the user/workstation 210; (3) the API 214 at the user/workstation 210 requests the proper application secret for the application 236 from the directory services 202a; (4) in response, the directory services 202a sends the encrypted application secret; and (5) the user/workstation 210 decrypts and forwards the property application secret to the application 236. Perlman, col. 6, lines 18-40. Thus, Perlman discloses that the user/workstation 210 is central involved in the various authentication processes, so that

the user/workstation 210 – and not a separate host – is the entity that forwards the application secrets to the controlled applications 236.

The reason for this deficiency is readily understood once the purpose of Perlman is taken into account. Rather than being concerned with granting access to controlled resources on the Internet, such as legacy applications (as is the case the Applicant's invention), Perlman's invention is directed to verifying the presence of a user when authenticating the user to different applications by providing each user with a hashed password value that is stored at the user's workstation "so that it may be readily accessible for authenticating the user to other applications of the system." Perlman, Abstract. Thus, the user/workstation is obtaining and forwarding authentication data to the application, not the host which performed the separately-recited "receiving," "extracting," and "decrypting" steps.

As seen from the foregoing (and putting aside for the moment the propriety of combining the Perlman and Wood references), a *prima facie* case of obviousness has not been established because neither Perlman nor Wood disclose or suggest a host that forwards the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource. Accordingly, claims 1, 14 and 25 are allowable. To the extent that dependent claims 3-6, 16-19 and 27-30 each respectively incorporate the requirements of independent claims 1, 14 and 25, these dependent claims are likewise allowable, even though there are additional differences recited in the dependent claims. For example, claims 4, 17 and 28 each variously recited "authenticating the client for access to the controlled resource based on the authentication data." To meet this requirement of claims 4, 17 and 28, the Examiner cites Perlman col. 6, lines 32-33, which discloses that "this arrangement provides efficient authentication of a user to various application programs or systems in a distributed network without burdening the user or consuming considerable bandwidth…." While the cited passage refers generally to "efficient authentication," there is no reference to authenticating the client based on the "authentication data" that was extracted and encrypted as claimed.

In an Office Communication dated April 25, 2008, the Examiner stated that he "would like to clarify that the motivation to combine the system of Wood US 6,892,307 with the forwarding of Perlman US 5,892,828 because the forwarding allows authentication to various applications in a distributed system, and in light of new obvious standards in Teleflex v. KSR." While Applicant is not sure what to make of the Examiner's stated intention, there is really

nothing specific in this statement for Applicant to respond to. In addition, any "motivation to combine" evidence will not change the fact that none of the cited references, alone or in combination, disclose or suggest authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract and decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 1, 3-6, 14, 16-19, 25 and 27-30 over Perlman and Wood be withdrawn and that the claims be allowed.

B. Claims 2, 15 and 26 Are Not Obvious Over Wood, Perlman And Olden

In response to the rejection of claims 2, 15 and 26 as being obvious over Wood, Perlman and Olden, Applicant respectfully requests reconsideration and withdrawal of the rejection because, as explained above with reference to independent claims 1, 14 and 25, none of the references disclose or suggest authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract *and* decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client. Olden does not remedy this deficiency.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Putting aside for the moment to propriety of combining these three references, a *prima facie* case of obviousness has not been established because none of the Wood, Perlman or Olden references disclose Applicant's host-based authentication scheme for decrypting and forwarding authentication data to a "controlled resource" which authenticates the client based on the authentication data before allowing the client to access the controlled resource. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 2, 15 and 26 over Wood, Perlman and Olden be withdrawn and that the claims be allowed.

C. Claims 7, 20 and 31 Are Not Obvious Over Wood, Perlman And Butt

In response to the Examiner's rejection of claims 7, 20 and 31 as being obvious over Wood, Perlman and Butt, Applicant respectfully requests reconsideration and withdrawal of the rejection because, as explained above with reference to independent claims 1, 14 and 25, none of the references disclose or suggest authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate

host system to extract *and* decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974); In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Putting aside for the moment the propriety of combining these three references, a *prima facie* case of obviousness has not been established because none of the Wood, Perlman or Butt references disclose Applicant's host-based authentication scheme for decrypting and forwarding authentication data to a "controlled resource" which authenticates the client based on the authentication data before allowing the client to access the controlled resource. For at least the foregoing reasons, Applicant respectfully requests that the obviousness rejections of claims 7, 20 and 31 over Wood, Perlman and Butt be withdrawn and that the claims be allowed.

VIII. CLAIMS APPENDIX - 37 CFR § 41.37(c)(1)(viii)

A copy of the pending claims involved in the appeal is attached as Appendix "B."

IX. EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

None.

X. RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.

XI. CONCLUSION

A *prima facie* case of obviousness has not been established because none of the cited references discloses or suggests authenticating client accesses at a controlled resource (e.g., a legacy application) before granting client access to the controlled resource by using a separate host system to extract and decrypt authentication data from the client that is then forwarded to the controlled resource for authenticating the client. In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

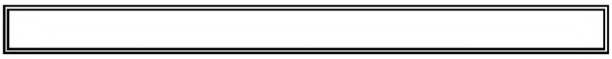
In view of the above arguments, it is respectfully urged that the rejection of the claims should not be sustained.

FILED ELECTRONICALLY
May 16, 2008

Respectfully submitted,

/Michael Rocco Cannatti/

Michael Rocco Cannatti
Attorney for Applicant



Reg. No. 34,791

APPENDIX A - RELATED APPEALS AND INTERFERENCES

There are no decisions rendered by a court or the Board in any related proceeding.

APPENDIX B - PENDING CLAIMS

1. (Previously Presented) A method for an authentication process within a distributed data processing system, the method comprising:

receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

2. (Original) The method of claim 1 wherein the controlled resource is a legacy application.

3. (Original) The method of claim 1 wherein the authentication data comprises a user identity and a password.

4. (Original) The method of claim 1 further comprising:

authenticating the client for access to the controlled resource based on the authentication data.

5. (Original) The method of claim 1, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the host.

6. (Original) The method of claim 1 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

7. (Original) The method of claim 1 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

8-13. (Canceled)

14. (Previously Presented) An apparatus for performing an authentication process within a distributed data processing system, the apparatus comprising:

receiving means for receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting means for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host;

and forwarding means for forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

15. (Original) The apparatus of claim 14 wherein the controlled resource is a legacy application.

16. (Original) The apparatus of claim 14 wherein the authentication data comprises a user identity and a password.

17. (Original) The apparatus of claim 14 further comprising:

authenticating means for authenticating the client for access to the controlled resource based on the authentication data.

18. (Original) The apparatus of claim 14, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the apparatus further comprising:

first parsing means for parsing the authentication data to retrieve a specific set of authentication data for the host.

19. (Original) The apparatus of claim 14 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the apparatus further comprising:

second parsing means for parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

20. (Original) The apparatus of claim 14 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

21-24. (Canceled)

25. (Previously Presented) A computer program product in a computer readable medium for use in a distributed data processing system for performing an authentication process, the computer program product comprising:

instructions for receiving an attribute certificate from a client at a host within the distributed data processing system;

instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

instructions for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

instructions for forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

26. (Original) The computer program product of claim 25 wherein the controlled resource is a legacy application.

27. (Original) The computer program product of claim 25 wherein the authentication data comprises a user identity and a password.

28. (Original) The computer program product of claim 25 further comprising:

instructions for authenticating the client for access to the controlled resource based on the authentication data.

29. (Original) The computer program product of claim 25, wherein the attribute certificate contains multiple sets of authentication data for multiple hosts, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the host.

30. (Original) The computer program product of claim 25 wherein the authentication data contains multiple sets of authentication parameters for multiple controlled resources, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the controlled resource.

31. (Original) The computer program product of claim 25 wherein the attribute certificate and the public key certificate are formatted according to an X.509 standard.

32-35. (Canceled)

APPENDIX C

1. A method for an authentication process within a distributed data processing system, the method comprising:

receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; **and**

forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

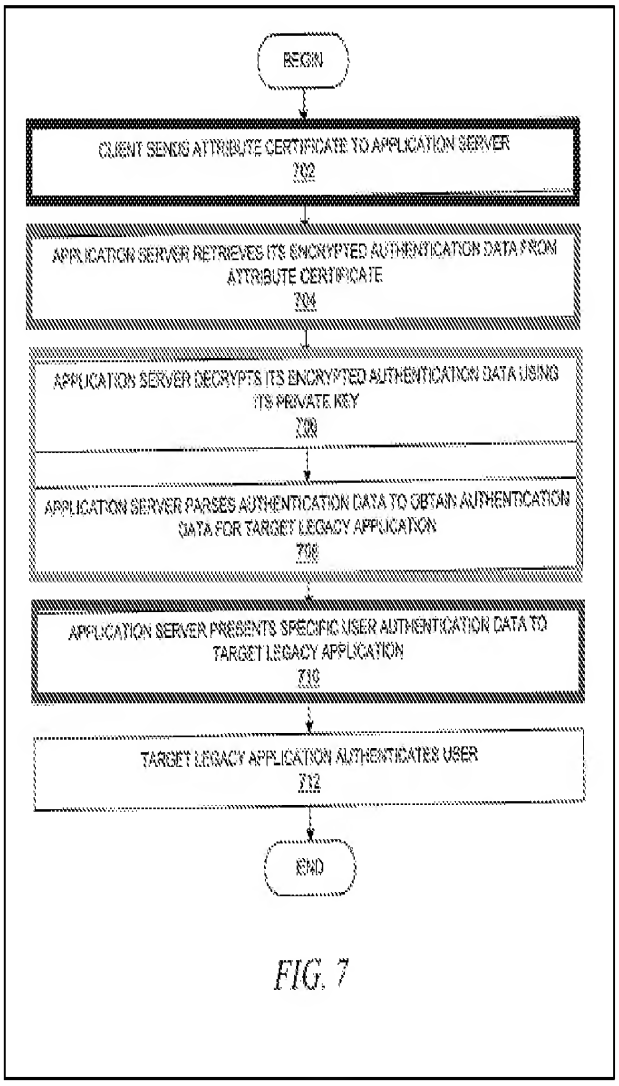


FIG. 7

14. An apparatus for performing an authentication process within a distributed data processing system, the apparatus comprising:

receiving means for receiving an attribute certificate from a client at a host within the distributed data processing system;

extracting means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

decrypting means for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

forwarding means for forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

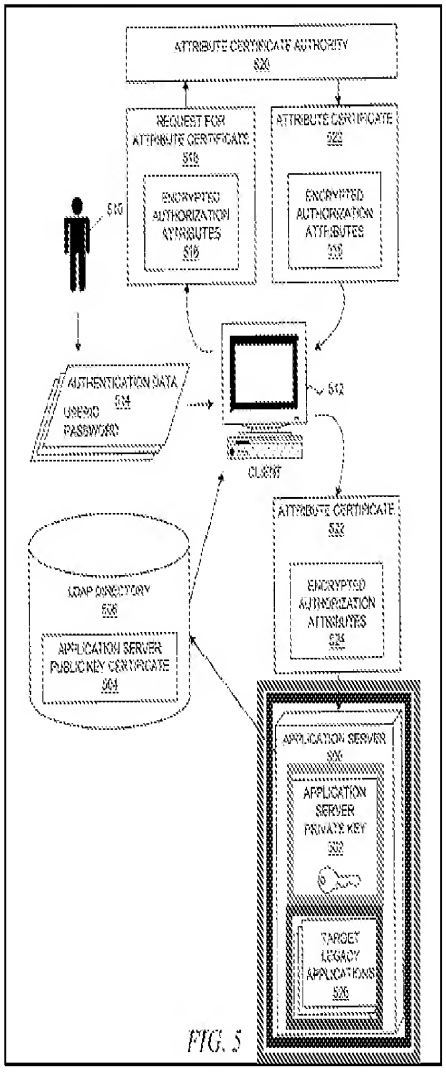


FIG. 5

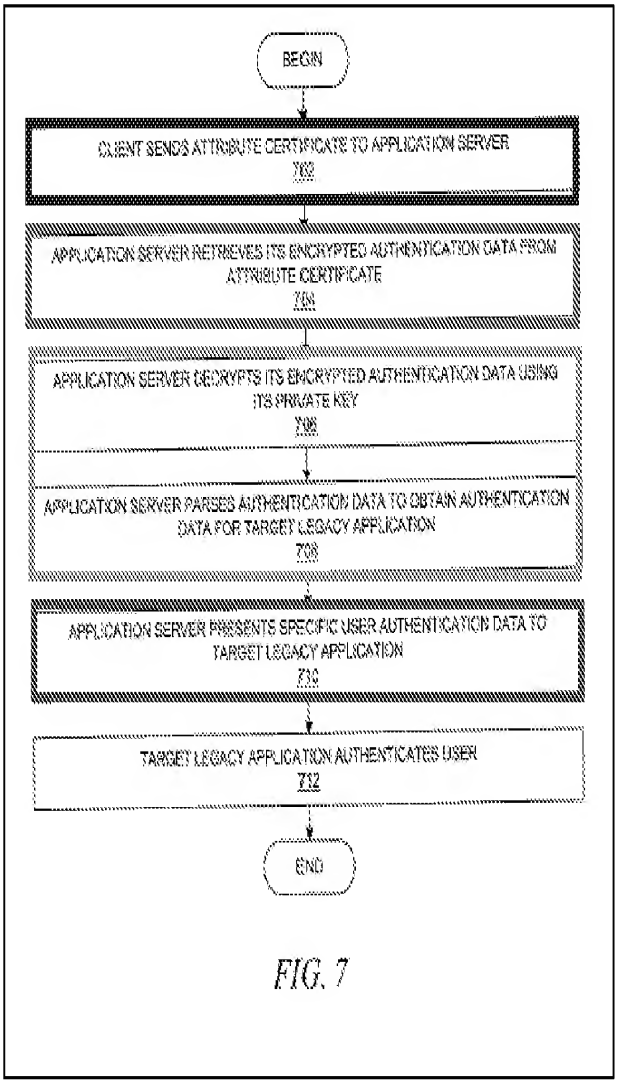


FIG. 7

25. A computer program product in a computer readable medium for use in a distributed data processing system for performing an authentication process, the computer program product comprising:

instructions for receiving an attribute certificate from a client at a host within the distributed data processing system;

instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the host;

instructions for decrypting the encrypted authentication data to regenerate the authentication data using a private key associated with the host; and

instructions for forwarding the authentication data to a controlled resource which authenticates the client based on the authentication data before allowing the client to access the controlled resource.

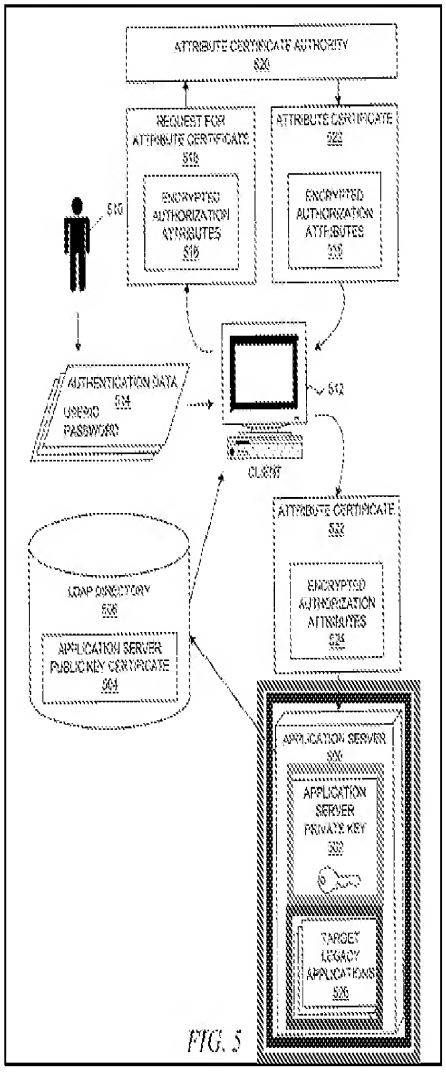


FIG. 5

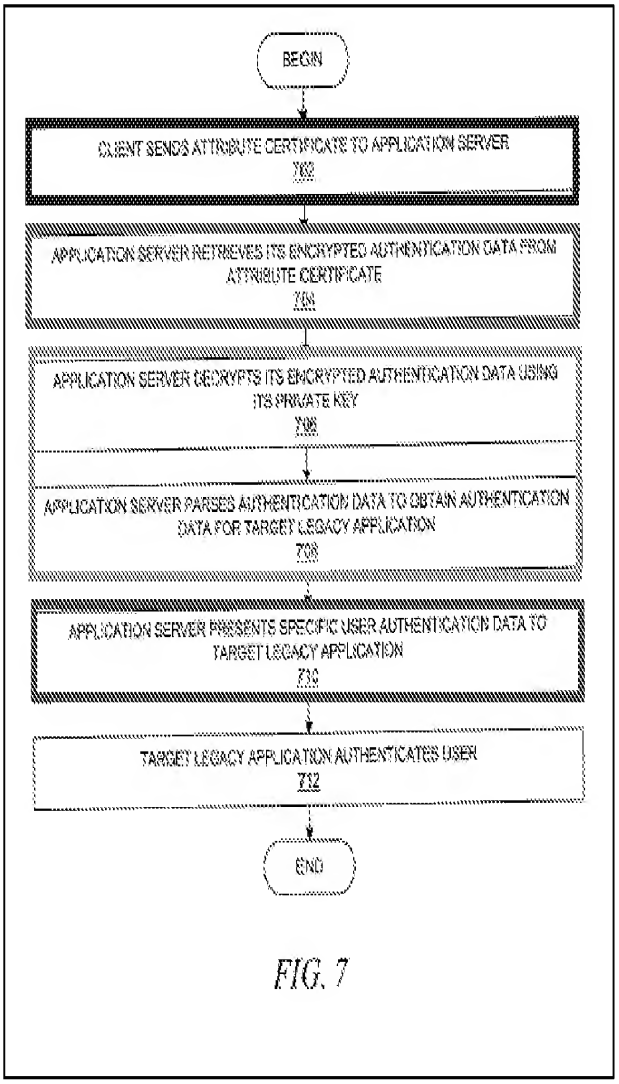


FIG. 7